QuintessenceLabs

Global Leadership in Quantum Communications

Enterprise Security Services incorporating Continuous Variable QKD

NASA Quantum Future Technologies Conference - 17 Jan 2012

Vikram Sharma, Founder & CEO

Presentation Structure

- **Motivation for an enhanced info sec architecture**
- **Technology layers**
  - Quantum Entropy Source
  - Quantum Key Distribution
  - Key Manager
  - Information Protection
- **Interop/Standards**
- **Technology Deployment**
- **Technology and Product Roadmap**

Threats to Cybersecurity Today

Vulnerability: Advances in adversary capability

- **Cyber breaches will occur**
  - Some vulnerabilities will always be present
    - Humans, manual processes, software faults
  - Windows of opportunity always present
    - Zero day vulnerabilities, patch implementation time > 0
- **Increased frequency and sophistication of attacks**
  - Evolution from 'whiz kids' to state sponsored activity
- **Current Info Security premised on one or more assumptions:**
  - **Efficient mathematical** attacks will never be feasible
  - **Computing resources** will never be sufficiently powerful for brute-force attacks
  - New technologies such as **quantum computers** will never be developed to sufficient scale
  - **Public Key Infrastructure/Trusted Third Parties** will always be secure from attack
- **Risk: If any one of the above invalidated, much of today's security infrastructure will be compromised**
  - **'Long lived' data** particularly at risk

Applied Quantum Technology

Protection of Valuable Information Assets

- **Leverage QKD capabilities**
  - Offer fundamental differentiator for key generation & distribution
- **Incorporate into comprehensive data security solution**
  - Protect data at-rest, in-transit and in-use
- **Can offer protection that is future-proof**
  - One Time Pad cipher
  - Secure from advances in adversary computational and mathematical capability
- **Can be architected into infrastructure of networks**
  - Optical layers can be designed into networks
- **Security not compromised if design/algorithms are revealed**

Technology Architecture

Four Functional Levels

- Embeddable KM libraries enforcing security policy
- Link and network encryption
- One-time pad cipher support
- Third party device and application support

- Secure key lifecycle management
- Cryptographic policy and control
- Separation of duty
- Authentication, logging and audit
- OASIS KMIP interface

- Continuous variable QKD
- Fibre optic and free space (planned) media
- Optional implementation levels to suit environment

- Quantum entropy source
- Optical and electronic hardware true RNG
- Very high speed

QUANTUM ENTROPY SOURCE

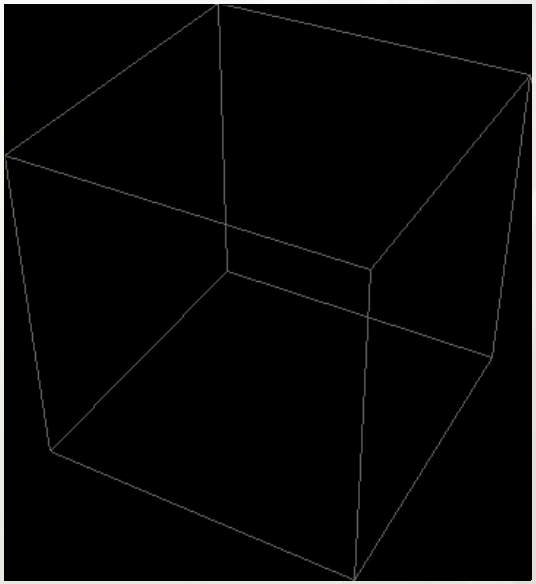
Quantum Entropy Source

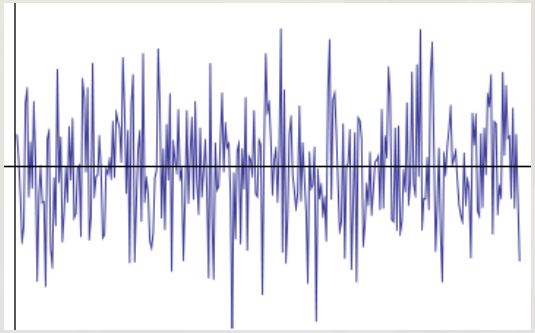
True Random Number Generator

- **Desirable characteristics**
  - Pass all randomness testing suites
  - Fast generation rate
  - Small form factor, cost effective

- **Vacuum state:**
  - space absent of particles, photons
- **But…**
  - contains energy
  - fleeting electromagnetic waves and particles
  - quantum state of light

- **Measure using homodyne detector**

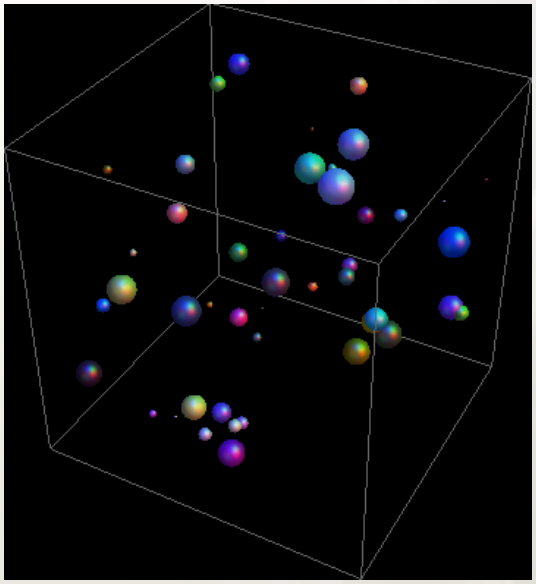


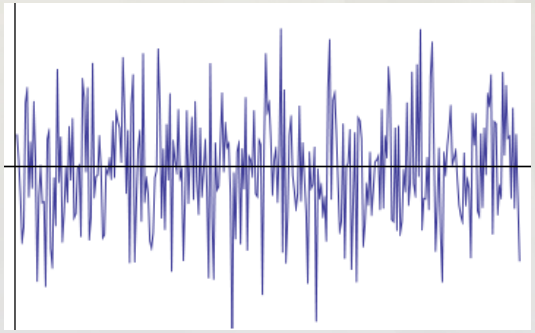


Quantum Entropy Source

True Random Number Generator

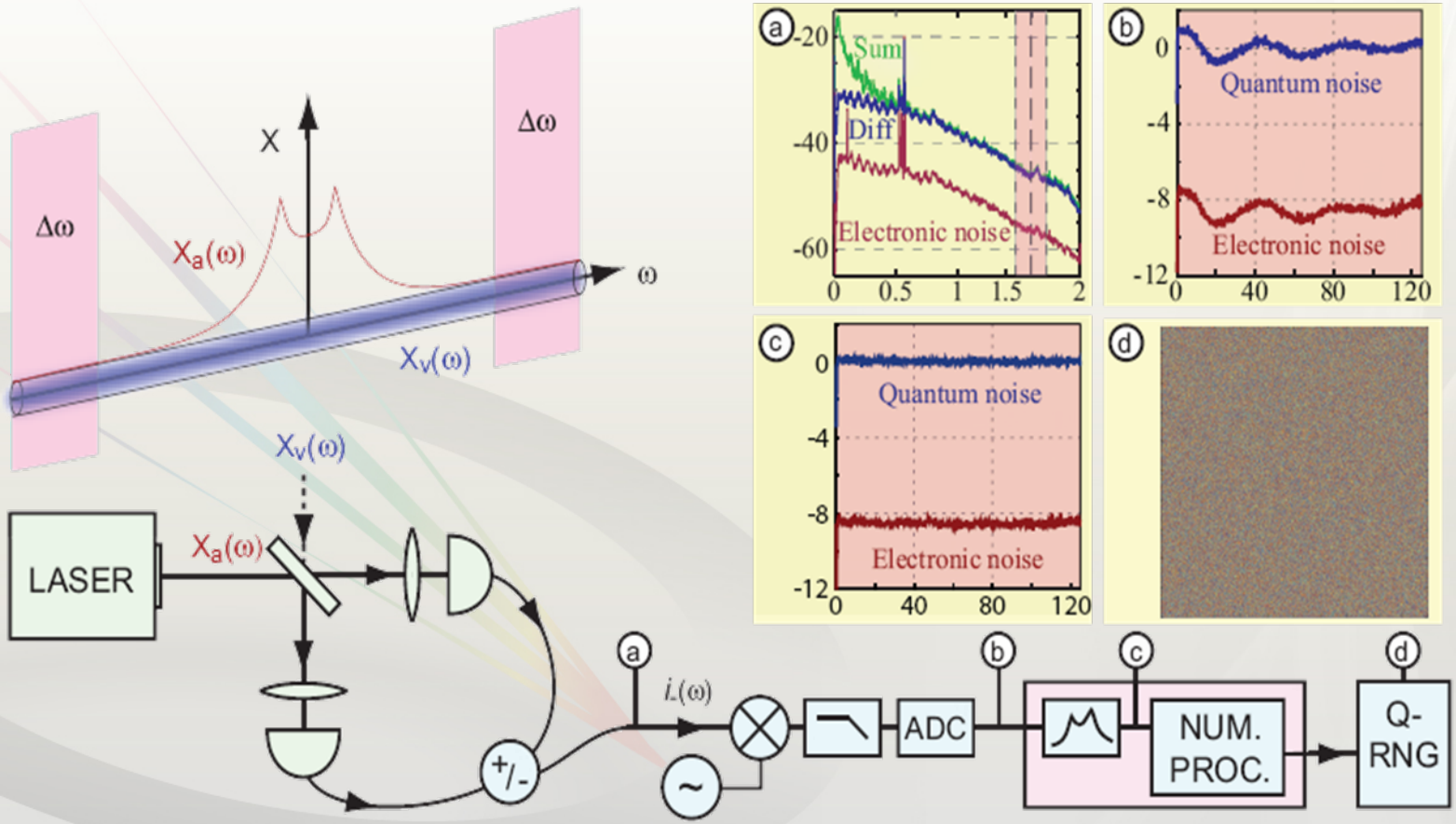
- **Desirable characteristics**
  - Pass all randomness testing suites
  - Fast generation rate
  - Small form factor, cost effective
- **Vacuum state:**
  - space absent of particles, photons
- **But…**
  - contains energy
  - fleeting electromagnetic waves and particles
  - quantum state of light
- **Measure using homodyne detector**





Quantum Entropy Source

Implementation

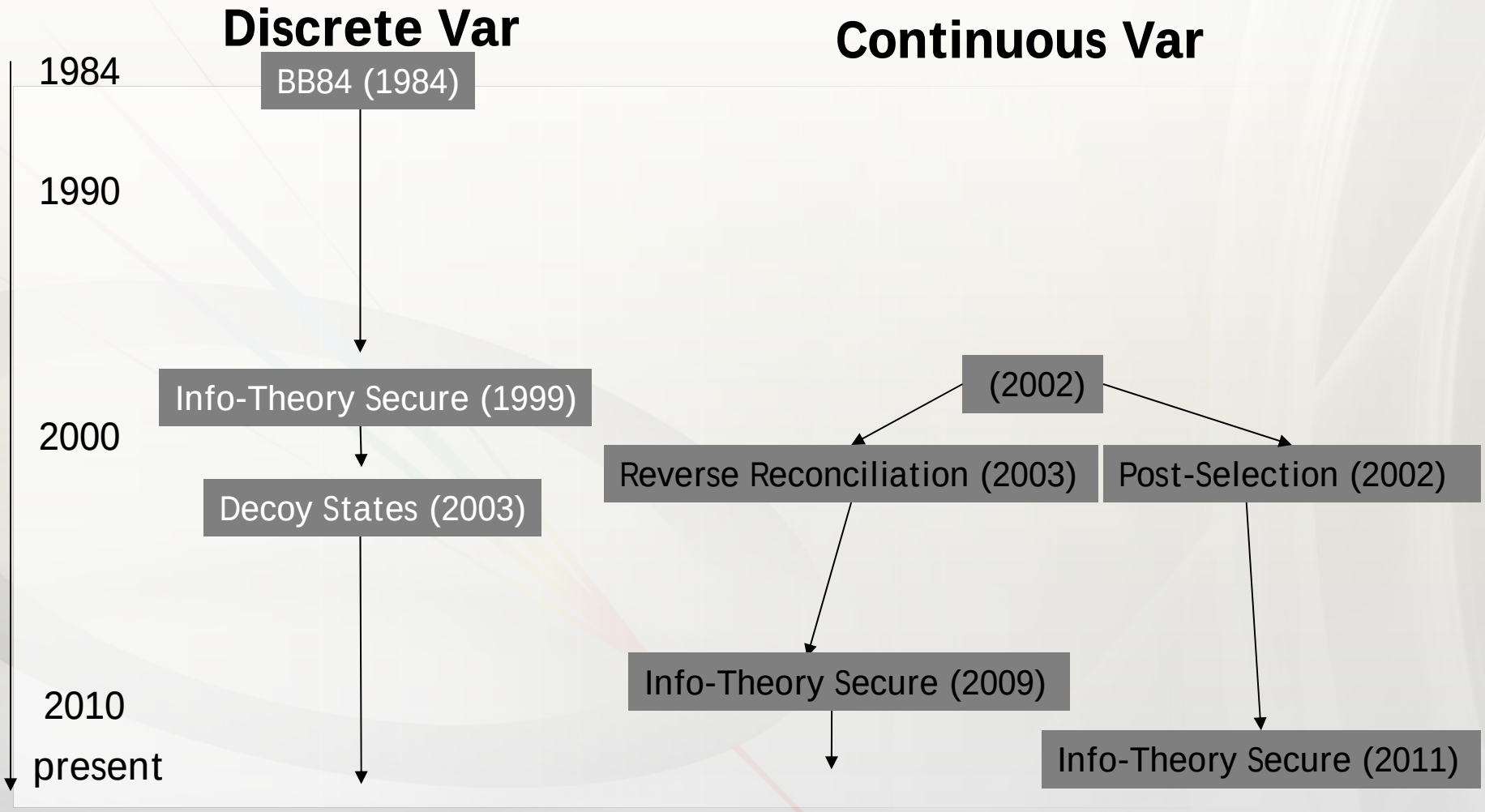


- 2 Gbit/s achieved
- Passes NIST & Dieharder tests

QUANTUM KEY DISTRIBUTION

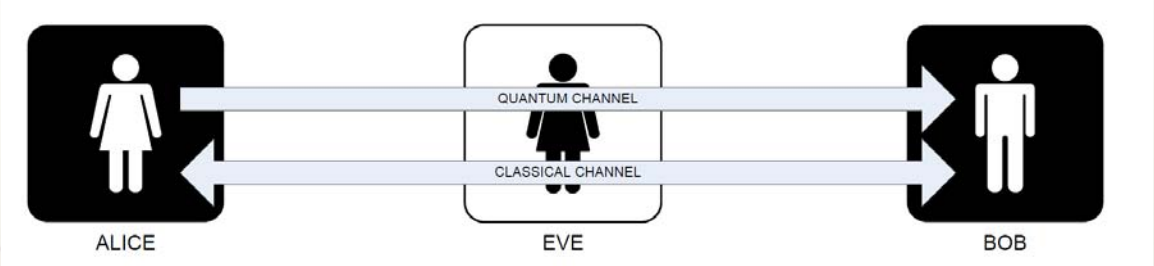
Quantum Key Distribution

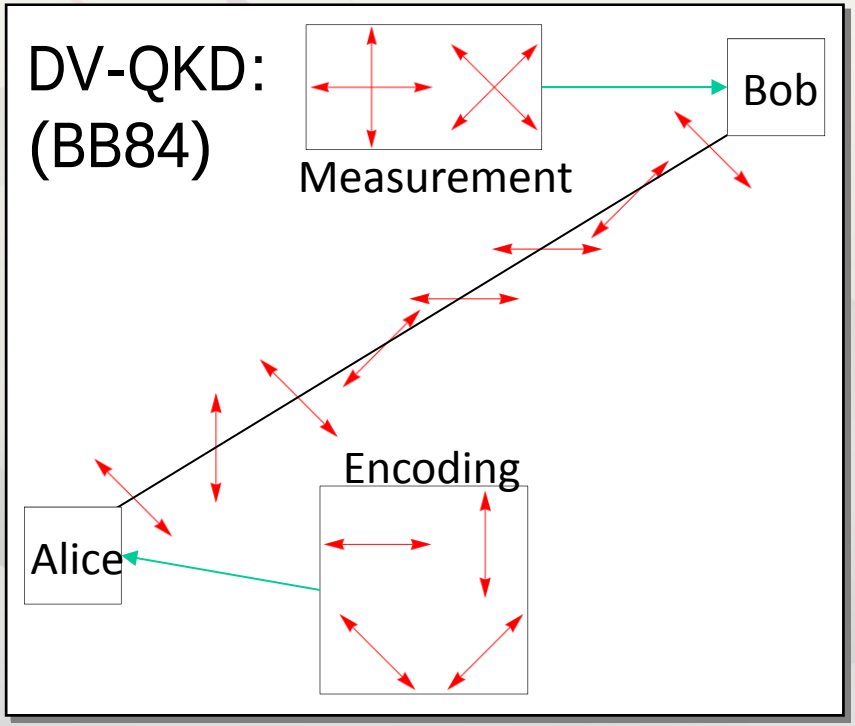
Some key theoretical developments

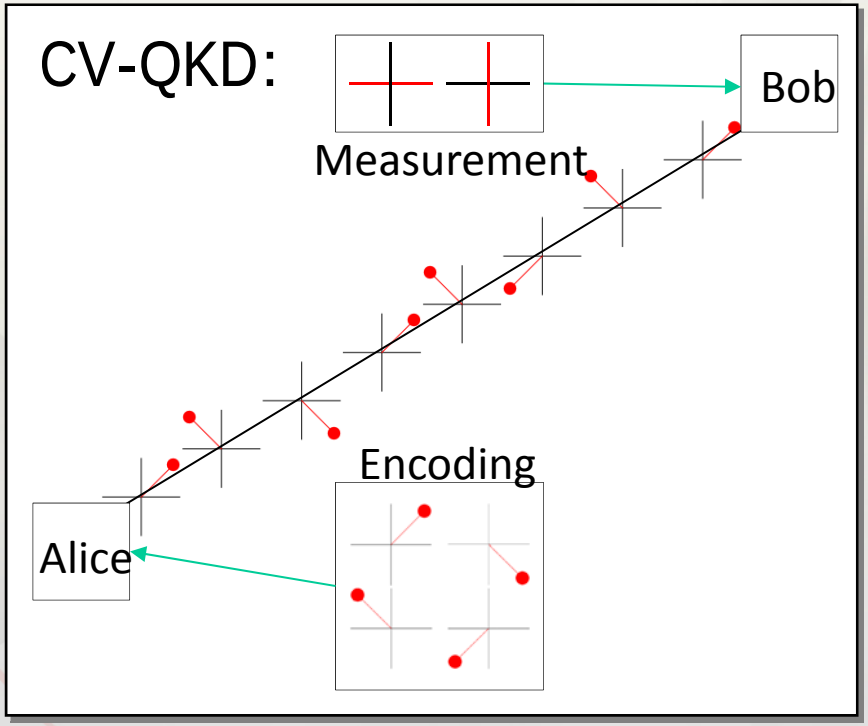


Quantum Key Distribution

Two approaches

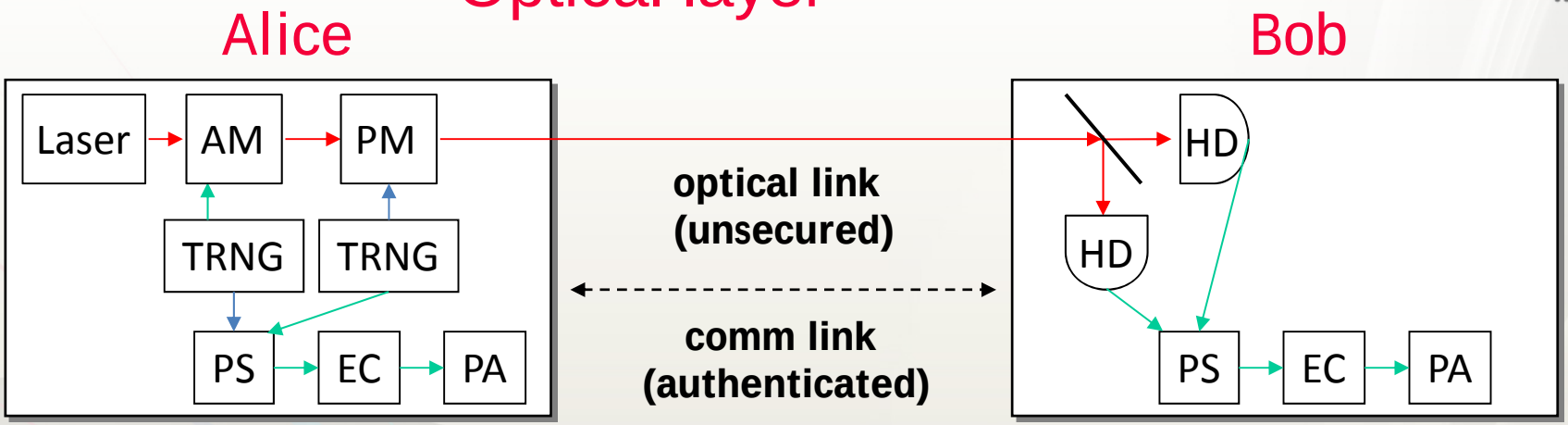






Quantum Key Distribution

Optical layer



- **Alice**
  - Generates string of random data bits (TRNG)
  - Prepares & transmits displaced coherent states (AM & PM)
- **Bob**
  - Measures **both** amplitude and phase quadratures (2xHD)
- **Alice & Bob**
  - Determine Eve's information (random 50% of data)
  - Post-selection (PS)
  - Error correction (EC)
  - Privacy amplification (PA)

Quantum Key Distribution

CV characteristics

- High detector efficiencies
- Off-the-shelf components
- Telecommunications compatible
- High-bandwidth

	Optical Device	Bandwidth
Laser	Shot-noise-limited laser	Essentially unlimited
Modulators	Amplitude and phase modulators	Currently: 10 GHz Available: 40 GHz
Detectors	Shot-noise-limited homodyne detectors	Currently: 10 GHz

KEY MANAGEMENT

Key Management

Quantum Key Manager

- **Manages cryptographic key and related material**
  - Distributed, information-theoretic secure key generation
  - Key policy management
- **Provides secure key distribution**
  - Authenticates access requests
  - Logs access requests
- **Is simple to use**
  - OASIS KMIP interface
  - Vendor neutral

OASIS KMIP TC Members

American Express
Axway Software
CA Technologies
Credant Technologies, Inc.
Cryptsoft Pty Ltd.
Election Systems & Software
EMC
Emulex Corporation
EURECOM
Freescale Semiconductor, Inc.
Hewlett-Packard
IBM
IECA, Inc.
Lexmark International Inc.
M.I.T.

OASIS KMIP TC Members

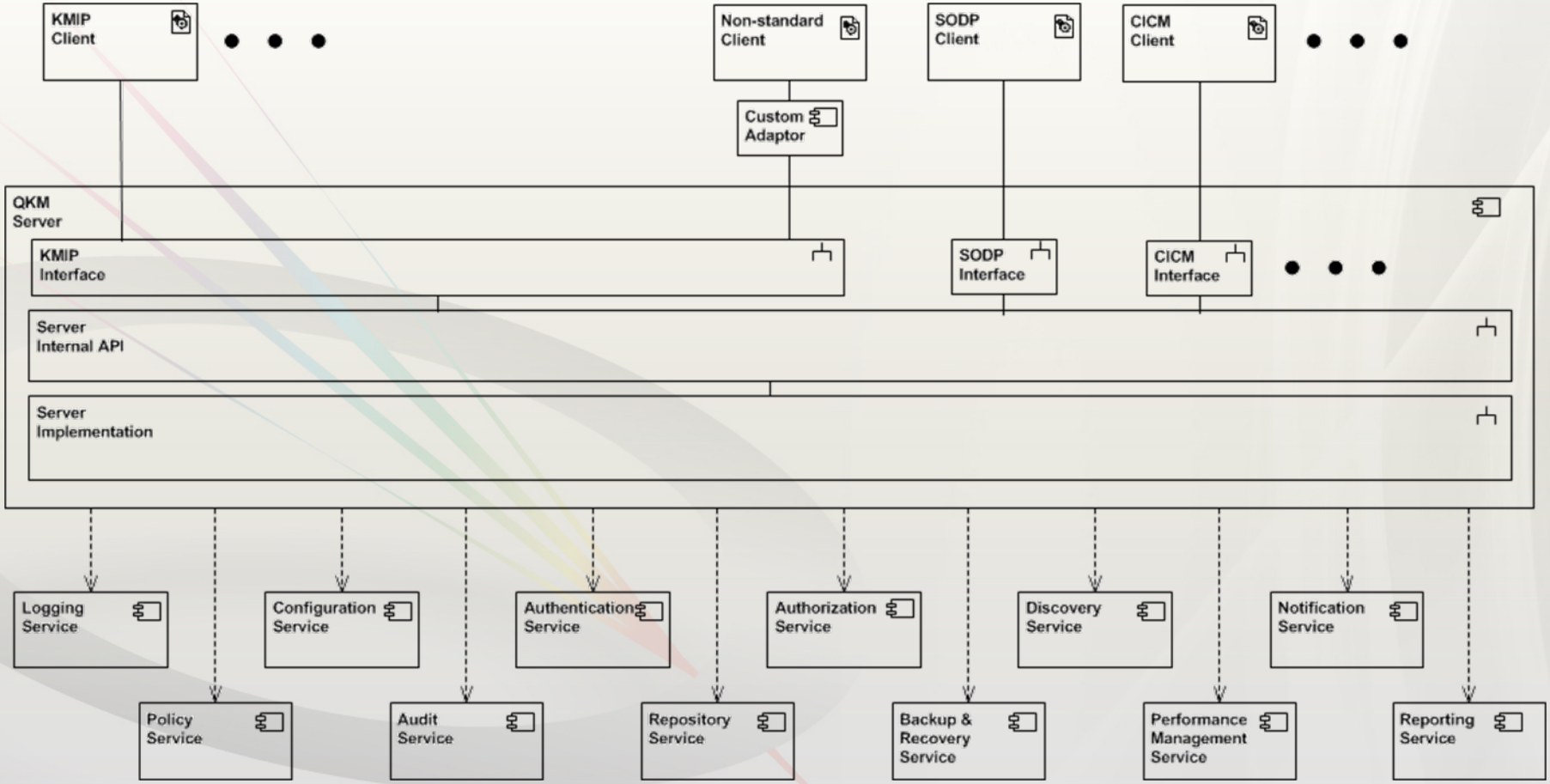
Mitre Corporation
National Security Agency
NetApp
NIST
Oracle
PrimeKey Solutions AB
Quantum Corporation
QuintessenceLabs Pty Ltd.
Red Hat
SafeNet, Inc.
Skyworth TTG Holdings Limited
Symantec Corp.
Target Corporation
Thales e-Security
UNH Interoperability Laboratory
Venafi, Inc.
Voltage Security
Vormetric, Inc.

Key Management
Applications

- **Mobile, network, application, database, file system, and storage encryption applications**
  - Tape library
  - Disk array
  - Storage area network
  - Database
  - Removable storage
    - e.g. flash drive, portable hard drive
  - Retail and hospitality (POS, PCI)
  - Financial (inter-bank, ATM, stock exchange)
  - Health
  - Enterprise
  - Network
  - Third party encryption products

Key Management

Component Architecture



INFORMATION PROTECTION

Information Protection

Data Centric Security

- **Improving protection**
  - How can the target of an attack be better protected?
  - Can we add a second highly secure layer of defence to the data?
- **When data is transmitted over an uncontrolled network it is encrypted**
  - Is it encrypted when transmitted and stored on controlled infrastructure?
  - Is the controlled infrastructure secure? Is it as secure as it should be?
  - Often, it is not encrypted on “controlled” infrastructure
    - And what about on “cloud” infrastructure?
- **A second layer of defence can be added**
  - Encrypt the data at all times: when stored, and when in transit
  - Centralise security policy enforcement for access to data
  - Log and monitor all data access requests and movement
  - At least two independent, but co-operating systems must be breached to access the data
    - The data on its own has no value because it cannot be decrypted without the key(s)

Information Protection

Data ARITIU Model

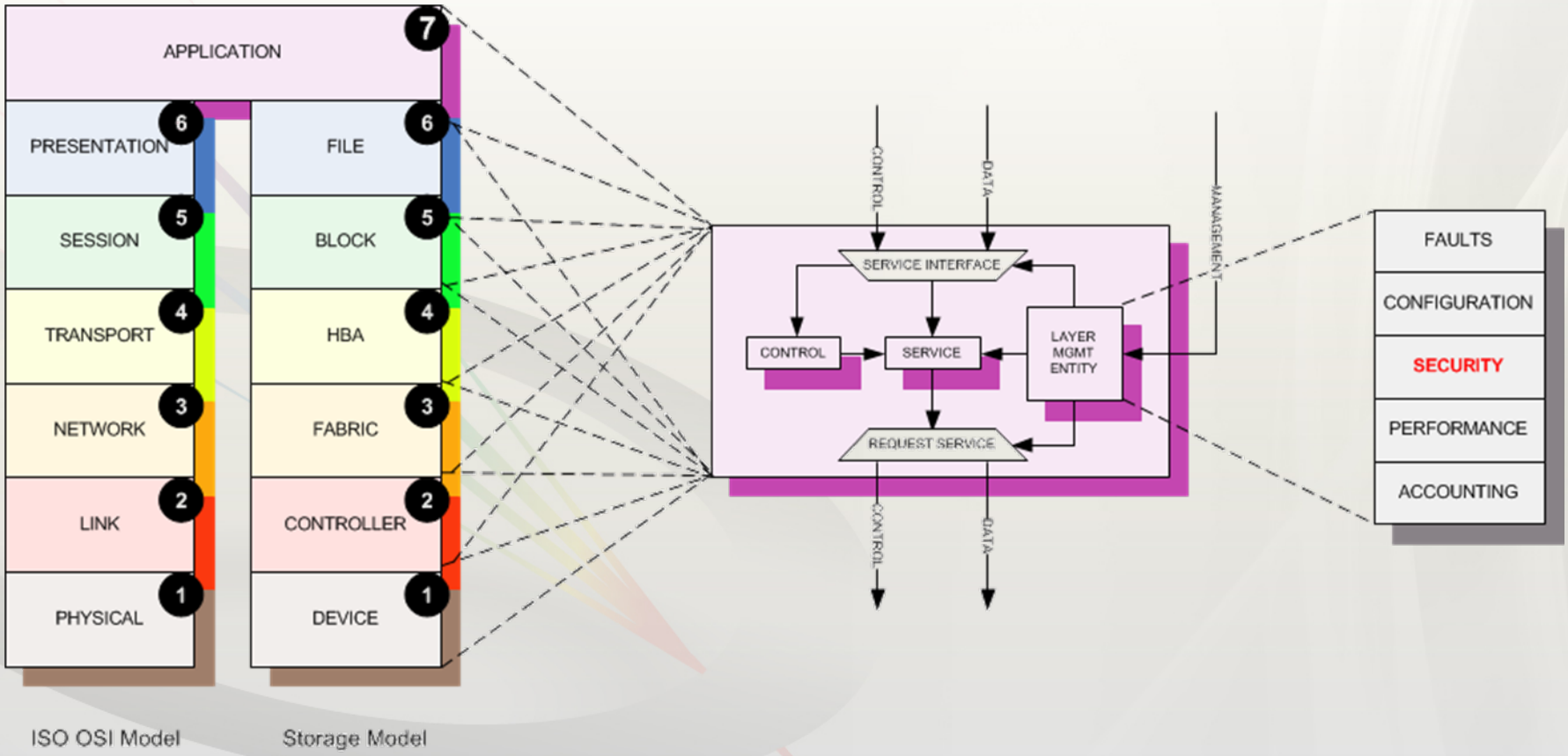
In-use

Operates on data transferred over a network. Examples: email, file transfer, web, remote DB, backup, electronic banking, e-health, and electronic tax filing.	7 APPLICATION	Operates on data in files and directories. Examples: documents, images, database, audio, video, file transfer, email attachments, libraries, and archives.
Data representation, encryption and decryption, convert machine dependent data to machine independent data.	6 PRESENTATION	6 FILE — Operating system file systems. Provides applications with logical view of files and directories. Controls application access to files and directories.
Inter-host communication, managing sessions between applications.	5 SESSION	5 BLOCK — Operating system drivers. Interfaces to host bus adaptor. Operates at block level. Issues and responds to device commands, as well as handling data.
End to end connections, reliability and flow control.	4 TRANSPORT	4 HBA — Physical and electrical interface to storage network or direct attached devices. Concerned with physical attachment, signal conditioning, and data formatting.
Path determination and logical addressing.	3 NETWORK	3 FABRIC — Physical layer interconnection between hosts and storage devices. May provide logical to physical mapping services, and pass-through data services.
Media access control and physical addressing.	2 LINK	2 CONTROLLER — Physical device control. Issues and responds to physical device commands. Provides physical and electrical device interfaces. Maps physical to logical.
Media, signal and binary transmission.	1 PHYSICAL	1 DEVICE — Storage device, including drive electronics. Examples: magnetic disk, tape, optical storage (CD-ROM, DVD), flash memory..

In-transit | At-rest

Information Protection

Security Policy Interface



INTEROP & STANDARDS

Interop/Standards

- OASIS KMIP
- NIST SP 800-57 Part 1
- AES, DES, RSA, ECC, HMAC, …
- SNMP, SSH, HTTP/TLS
- FIPS 140-2
- NIST, Diehard, Dieharder
- IEEE 802.1D

Interop/Standards

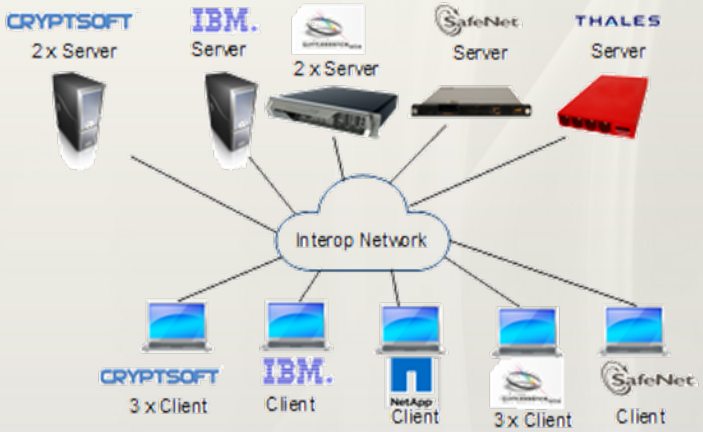
Successful Key Management Deployment

OASIS
Advancing open standards for the information society

ORACLE CRYPTSOFT

SafeNet ca technologies hp NIST EMC²

THALES IBM symantec



Interop/Standards

KMIP Interop Tests

- **Successful interoperability tests performed with IBM, Zurich**

```
# Wed Jan 11 14:43:05 EST 2012
#--TEST_EXE:BEGIN:v1_1-uc3_1_3--#
test_exe.sh: v1_1-uc3_1_3 -h
fondue.zurich.ihost.com -p 9191 -i -k
keys/client.pem.ibm -c keys/root.pem.ibm
Connecting to server...
Sending KMIP create (symmetric key)
request...
Receiving KMIP create response...
Response status: KMIP_RESULT_SUCCESS
Key UUID: 47c211be-20e3-4f22-944f-
6a2b7e81f650
Sending KMIP locate request...
Receiving KMIP locate response...
Response status: KMIP_RESULT_SUCCESS
UUID Count: 1
Key UUID: 47c211be-20e3-4f22-944f-
6a2b7e81f650
```

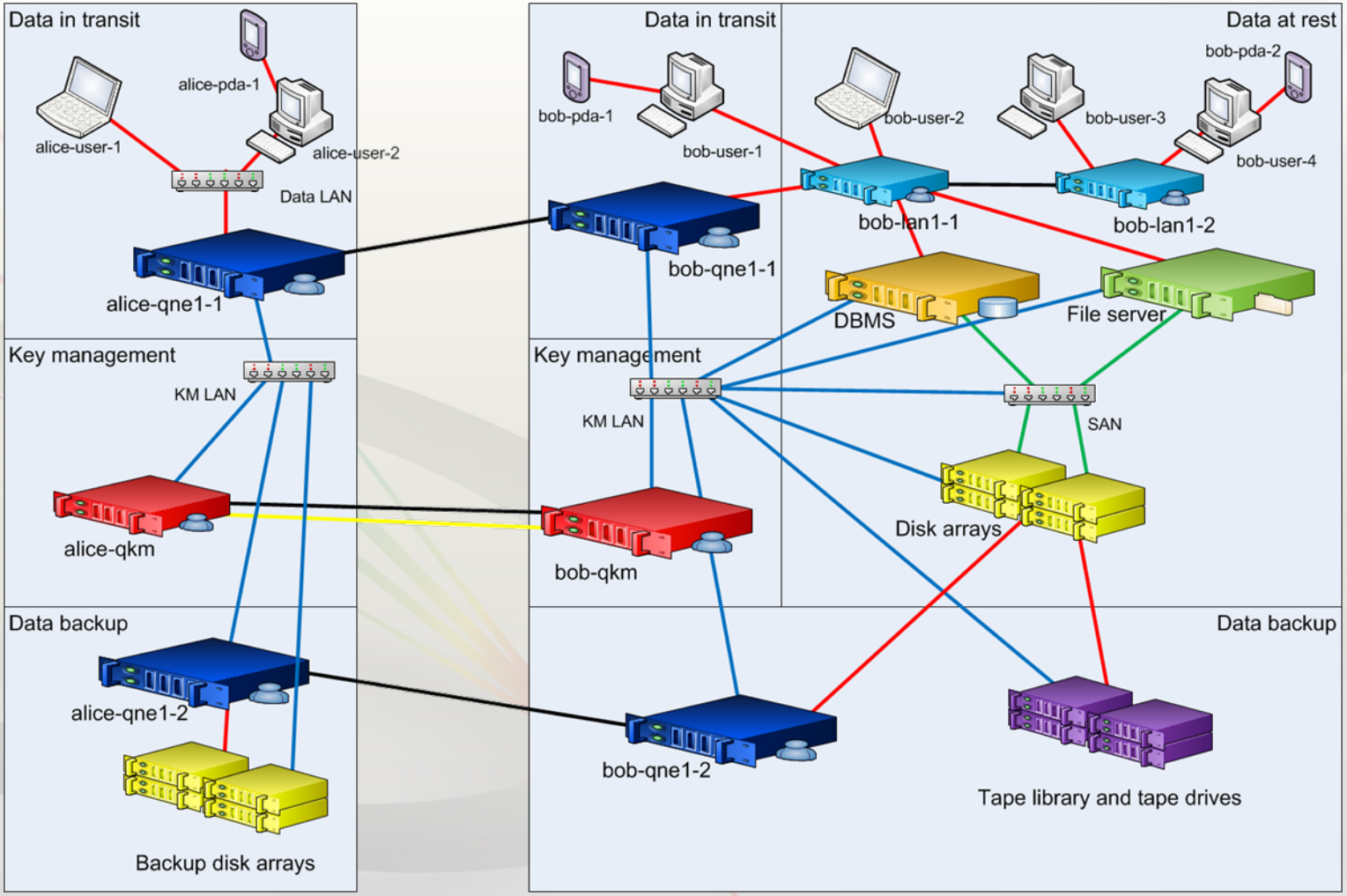
```
Sending KMIP get (symmetric key)
request...
Receiving KMIP get response...
Response status: KMIP_RESULT_SUCCESS
Sending KMIP destroy (key) request...
Receiving KMIP destroy response...
Response status: KMIP_RESULT_SUCCESS
…

Disconnecting...
Finished
Exit code 0
TEST:SUCCESS: v1_1-uc3_1_3
#--TEST_EXE:END:v1_1-uc3_1_3--#
# Wed Jan 11 14:43:10 EST 2012
```

- **Interoperability demo at RSA Conference 2012**

TECHNOLOGY DEPLOYMENT

Deployment Con Ops

Heterogeneous IT Environment

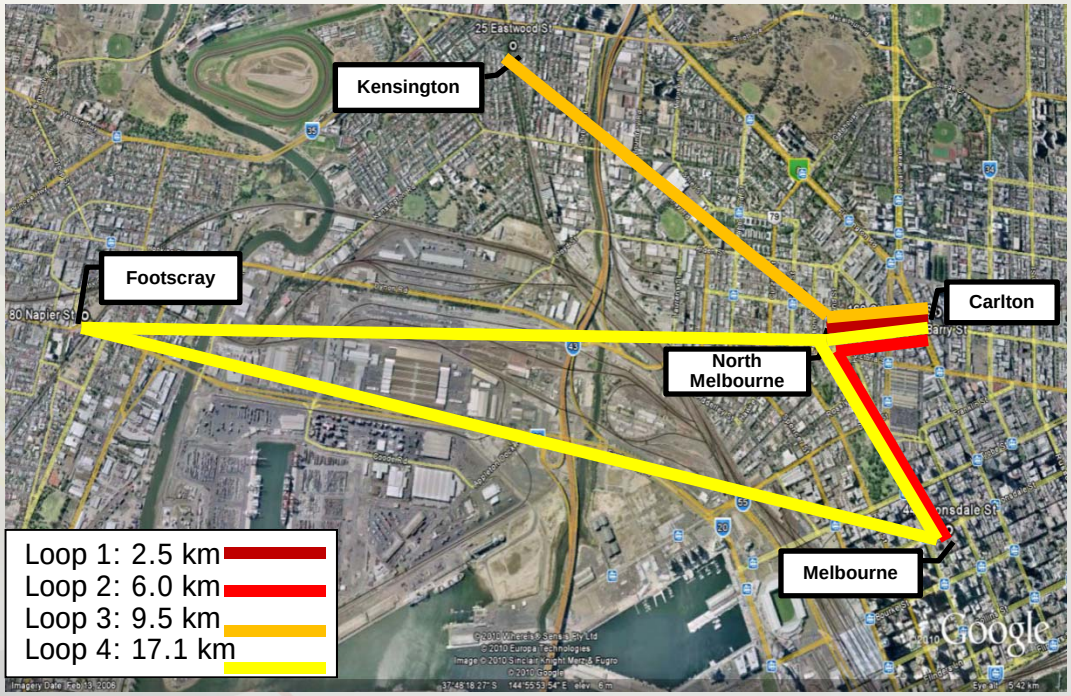


Successful Deployment

Telstra

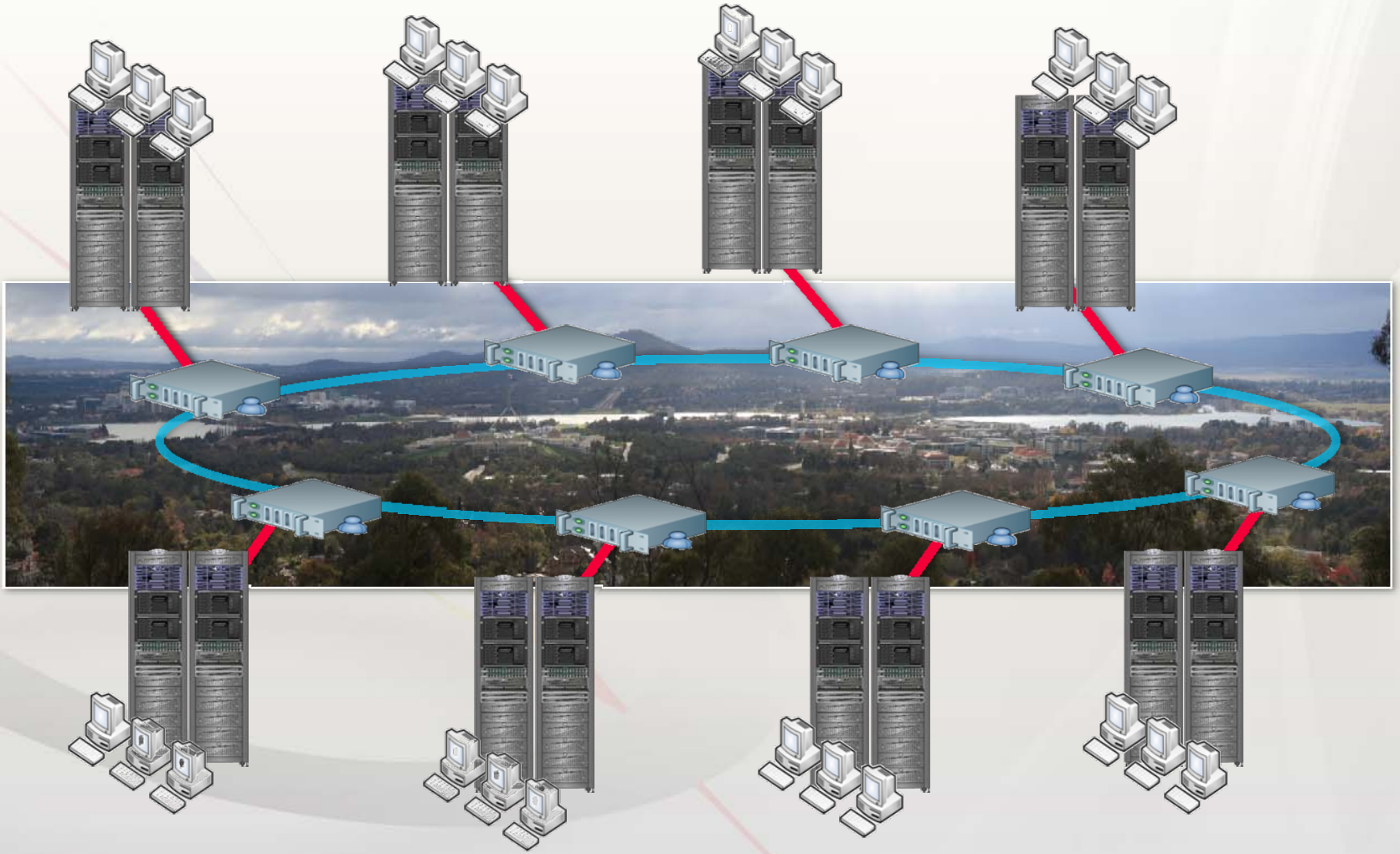
November 2010

- **Link encryption over commercial optic fiber**
  - Telstra Integration Labs
  - Varied fiber routes in Melbourne, Australia
  - Range of environmental conditions



Proposed Deployment

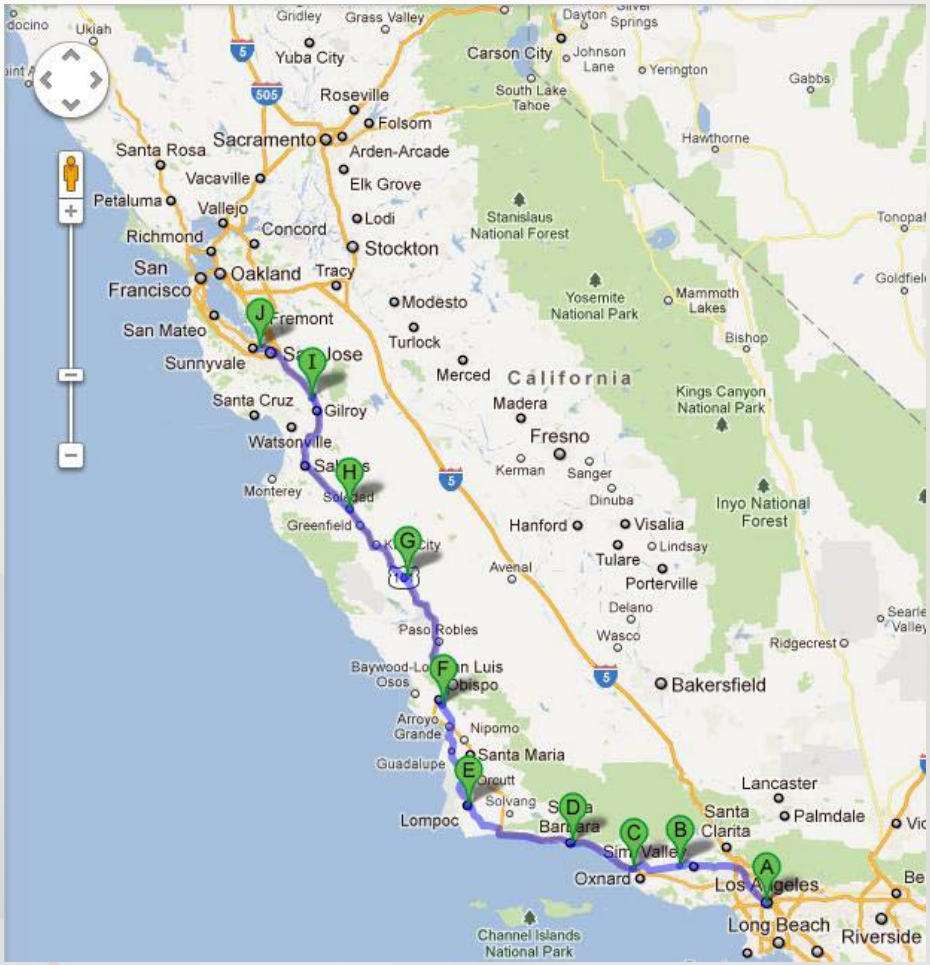
Ultra-secure quantum network in Canberra



Proposed Deployment

NASA/JPL

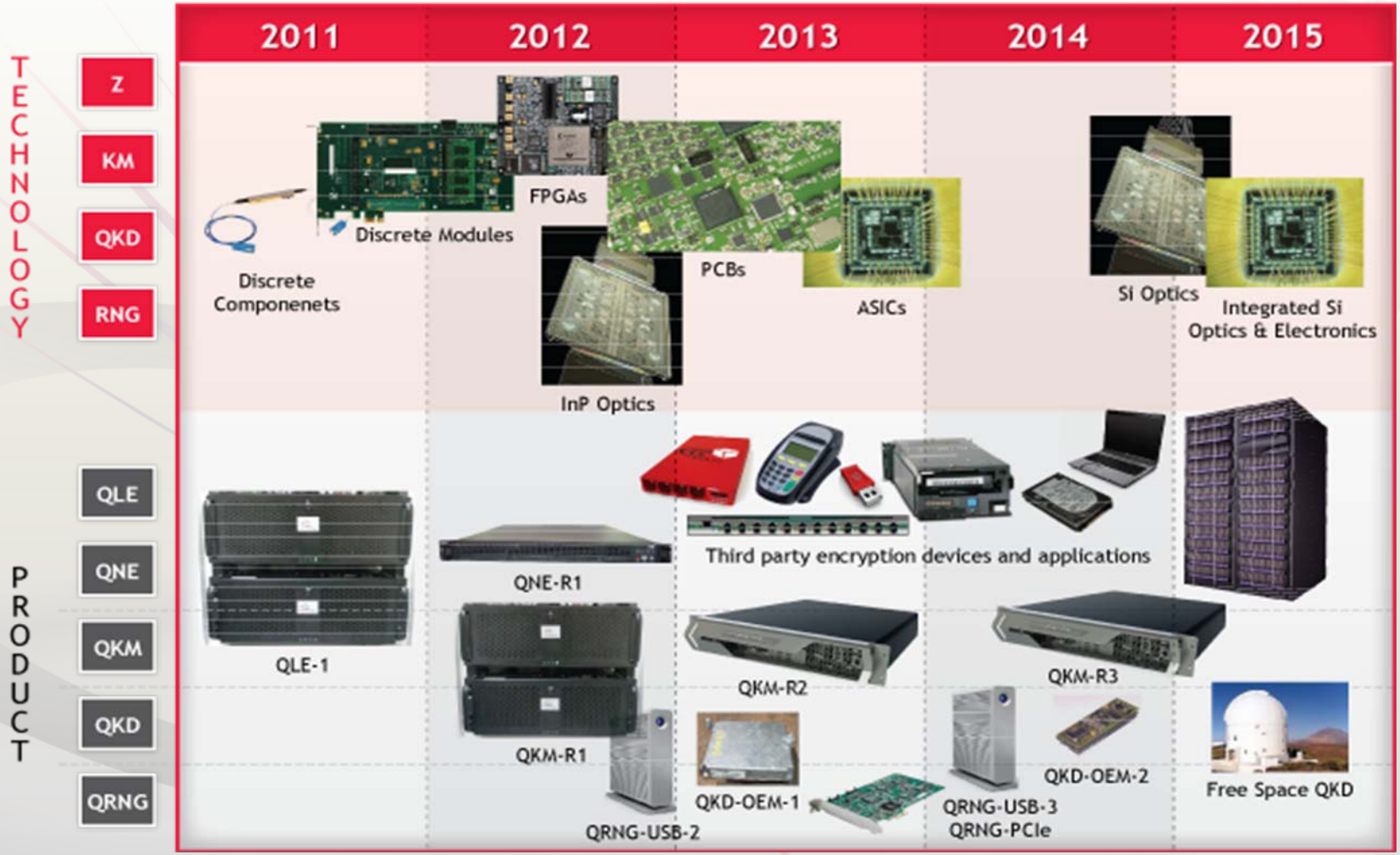
- **Prototype unconditionally secure communications network, spanning terrestrial and space links**
- **Phased project**
  - Terrestrial fiber
    - NASA Ames to JPL Pasadena
  - Terrestrial free space
  - Ground to aircraft
  - Ground to satellite
- **Colin Williams (JPL) to discuss in greater detail**



ROADMAP

Roadmap

Technology & Product



QuintessenceLabs

Global Leadership in Quantum Communications